In the claims:

Please cancel claim 7.

Please amend claims 1-5, 9, and 11-16 as follows:

1. (currently amended) A secure transaction system, comprising:

a plurality of information carriers distributed to authorized users for secure storage of information related to carrying out of transactions by said authorized users, each information carrier having a passive data storage medium but lacking any data processing unit, said information stored on said passive data storage medium being in encrypted form and including transaction messages, crytographic keys, digital signatures and at least one digital certificate issued to an authorized user; and

a tamper-resistant drive for reading and writing information relating to transactions on an information carrier presented thereto by an authorized user, said tamper-resistant drive connected via a communications link or network to a host computer, said tamper-resistant drive having a control unit executing secure protocols for mediating communication between said host computer and tamper-resistant drive and between said tamper-resistant drive and information carrier, said tamper-resistant drive also having a cryptographic processing unit providing encryption and decryption of transaction messages and digital certificates in accord with said secure protocols executed by said control unit and using cryptographic keys, including cryptographic keys stored by said tamper-resistant drive and cryptographic keys read from said information carriers, as specified by said secure protocols.

2. (currently amended) The system of claim 1 wherein said [data] cryptographic processing unit of said tamper-resistant drive also providing, as specified by said secure protocols, encryption and decryption of information communicated with said host computer via said communications link.

3. (currently amended) The system of claim 1 wherein said tamper-resistant drive includes sensors detecting attempted intrusions into the tamper-resistant drive, said control unit being responsive to said sensors for destroying critical cryptographic keys in the tamper-resistant drive upon detection of any intrusion.

4. (currently amended) The system of claim 1 wherein said passive data storage medium on said information carrier comprises optical media.

5. (currently amended) The system of claim 4 wherein said information carrier is [on] an optical memory card.

6. (original) The system of claim 4 wherein said information carrier is an optical disk.

7. (cancelled)

8. (original) The system of claim 1 wherein said information stored on said information carrier is in encrypted form corresponding to a decryption key stored in said tamper-resistant drive.

9. (currently amended) The system of claim 8 wherein said information stored on said information carrier also includes personal data for generating cryptographic keys of said authorized user.

10. (original) The system of claim 9 wherein said personal data comprises any of a personal identification number (PIN), a password, and biometric data.

11. (currently amended) The system of claim 1 wherein said passive data storage medium is logically partitioned and at least one different digital certificate is stored thereon for each partition.

12. (currently amended) The system of claim 1 wherein said secure protocols include an enrollment of an authorized user wherein personal data for said user is digitally signed, and transmitted from a host computer to said tamper-resistant drive with at least one digital certificate, and recertified by said tamper-resistant drive and stored on said passive data storage medium.

13. (currently amended) The system of claim 1 wherein said secure protocols include a transaction by an authorized user wherein transaction requests and authorization information [and] are transmitted between said tamper-resistant drive and said host computer and between said tamper-resistant drive and said passive data storage medium with at least one digital certificate.

14. (currently amended) The system of claim 1 wherein said secure protocols executed by said tamper-resistant drive include at least one protocol that permits modification of said cryptographic keys stored by said tamper-resistant drive.

15. (currently amended) The system of claim 14 wherein said protocol permitting modification of said cryptographic keys is one of said secure protocols mediating communications between said host computer and said tamper-resistant drive.

16. (currently amended) The system of claim 14 wherein said protocol permitting modification of said cryptographic keys is one of said secure protocols mediating communication between said tamper-resistant drive and said information carriers.

17. (original) The system of claim 14 wherein at least one of said secure protocols also permits modification of the secure protocols themselves.